UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

NAKIA ROLLING, MARCUS MCDANIEL, KENNETH BRULINSKI, CHARMISSHA TINGLE, NICOLE PORTNOY, APRIL PIERCE, KELLY BRUNO, MICHAEL SUSSMAN, and TRACEY LUCAS, on behalf of themselves and all others similarly situated, Plaintiffs, vs. WAWA, INC., Defendant.	(Related to: *In Re Wawa, Inc. Data Breach Litigation*, Civ. No. 19-6019-GEKP) Case No. _____ Civil Action **COMPLAINT - CLASS ACTION**

Plaintiffs Nakia Rolling, Marcus McDaniel, Kenneth Brulinski, Charmissha Tingle, April Pierce, Kelly Donnelly Bruno, Nicole Portnoy, Michael Sussman and Tracey Lucas ("Plaintiffs"), on behalf of themselves and all others similarly situated, bring this class action complaint against Defendant Wawa, Inc. ("Wawa" or "Defendant"). Plaintiffs allege as follows upon personal knowledge as to their own acts and experiences, and upon the investigation of their attorneys as to all other matters.

I. INTRODUCTION

1. This is a data breach class action on behalf of millions of consumers whose credit and debit card information was stolen by cybercriminals as part of a massive cyber-attack on Wawa's payment card environment and systems. The data breach involved consumer transactions at all or most of Wawa's 850 convenience stores (including gas pumps) over a nine-month period. Information compromised in the breach included credit and debit card numbers, card expiration

dates, and cardholder names ("Card Information"). The window of the breach on Wawa's servers lasted from March 4, 2019 to December 12, 2019 (the "Data Breach").

2. As a result of the Data Breach, many class members have experienced and will continue to experience fraudulent credit and debit card purchases and other fraud related to their accounts. Class members will also incur out-of-pocket costs to purchase protective measures such as credit monitoring services, credit freezes, and credit reports. They will also incur costs for replacement cards and other items directly or indirectly related to the Data Breach.

3. All Plaintiffs have sustained actual, palpable fraud and injury as a result of the Data Breach. Plaintiffs and class members have also been exposed to a heightened and imminent risk of fraud and identity theft. They must now and indefinitely in the future closely monitor their financial accounts to guard against fraud. This is a burdensome and time-consuming process.

4. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Card Information was stolen in the Data Breach. Plaintiffs seek remedies including reimbursement of fraud losses and other out-of-pocket costs, compensation for time spent in response to the Data Breach, free credit monitoring and identity theft insurance beyond Defendant's current one-year offer, and injunctive relief involving substantial improvements to Defendant's card payment data security systems.

II. PARTIES

A. Plaintiffs

5. Plaintiff Nakia Rolling is an adult residing in Cheltenham, Pennsylvania. On November 29, 2019, Ms. Rolling discovered that her Bank of America debit card had been used that same day to make a fraudulent purchase in the amount of $322.29. Ms. Rolling contacted Bank of America that same day to dispute the charge. Bank of America closed her checking account and opened her a new checking account. Bank of America reissued Ms. Rolling a

replacement debit card, but it took several days before she received it in the mail, during which she was without the benefit of using her debit card to conduct everyday transactions. Furthermore, although Bank of America reimbursed her for the fraudulent charge, it did not do so for 7-10 business days. During that time, Ms. Rolling was without the funds used to make this fraudulent charge. Ms. Rolling uses her debit card for everyday personal transactions, but also uses it for expenses for her hair styling business. As a result, Ms. Rolling has suffered immense frustration, aggravation and loss of time traveling to her bank, discussing this situation with her bank, disputing the fraudulent charge, and changing her card information with every vendor that automatically deducts bills and expenses—both personally and for her business—from her account on a recurring basis. Ms. Rolling estimates that she has already spent approximately two hours engaging in the foregoing remedial actions, and continues to spend additional time and effort further contacting such vendors to change her payment information consistent with her new checking account. Furthermore, Ms. Rolling regularly monitors her credit using CapitalOne. After discovering the fraudulent charge, she checked her credit on CapitalOne and it informed her that her information is available on the black market. In response, she contacted Experian and Equifax and set up fraud alerts with both. Ms. Rolling suffered additional harm in the form of aggravation and lost time by checking her credit and contacting these two credit bureaus to set up fraud alerts. Prior to this fraudulent charge, Ms. Rolling has never previously suffered fraudulent activity on her Bank of America account.

6. Plaintiff Marcus McDaniel is a resident of Florida. He used his debit card at a Wawa location in Florida during the breach period. After using his debit card at Wawa, he suffered six fraudulent purchases on the same card. Specifically, on December 13, 2019, he experienced fraudulent charges of $1.60, $4.20, $1.10, and $2.10. On December 16, 2019, he experienced

fraudulent charges of $99.90 and $100.00. He disputed the charges with his bank. The dispute process was time-consuming and involved multiple phone calls with the bank, including calls while he was at work. The bank ultimately reversed the $1.60, $4.20, $1.10, and $2.10 charges, and it granted a "provisional credit" regarding the $99.90 and $100.00 charges. The provisional credit is subject to further review by the bank. The bank issued a replacement debit card, which took several days to receive. Plaintiff McDaniel had no convenient way to access his bank account funds in the meantime, which was particularly inconvenient during the holiday shopping season. Plaintiff McDaniel had never experienced any fraudulent charges on his debit card or bank account prior to the Wawa breach. To his knowledge, his debit card number or banking information were not involved in any other data breaches other than the Wawa breach. Had Mr. McDaniel known that Wawa does not take adequate steps to protect customer Card Information, or had Wawa disclosed to him that it does not, he would not have made purchases at Wawa.

7. Plaintiff Michael Sussman is an adult residing in Lakeworth, Florida. Mr. Sussman used his American Express credit card at affected Wawa locations during the Data Breach window. On December 4, 2019, Mr. Sussman was alerted by American Express about possible fraudulent activity on his credit card account. He immediately called American Express to gather more information on the fraudulent activity. American Express confirmed that the fraudulent charge was in the amount of $957 at Walmart. Refraining from disclosing the exact breach, American Express did comment to Mr. Sussman that many of their cardholders have had increased fraud incidents during that same week. As a result of the fraud, American Express canceled his existing credit card, the fraudulent charge was reversed, and Mr. Sussman was issued a new credit card. Mr. Sussman has spent approximately five hours addressing the fraud he experienced. Prior to being victimized by the Wawa Data Breach, Mr. Sussman's American Express credit card had never

been subjected to theft or fraud. Had Mr. Sussman known that Wawa would not adequately protect his Card Information and other sensitive information entrusted to it, he would not have made regular purchases at Wawa using his payment card. As a result of Wawa's failure to adequately safeguard Plaintiff Sussman's Card Information, he has been injured.

8. Plaintiff Kenneth Brulinski is a resident of Maryland. He used his debit card many times at one or more Wawa locations in Maryland during the breach period. After using his debit card at Wawa, he experienced four fraudulent purchases on the card. Specifically, on November 14, 2019, he experienced fraudulent charges of $44.99 and $67.93 from Hulu, a television streaming website. On November 27, 2019, he experienced fraudulent charges of $6.99 and $6.99, described on his bank statement as "Google * Little Bird Internet." He disputed the charges with his bank. The bank issued a "provisional credit" to reverse each of the four charges. The bank also cancelled his debit card and issued a replacement card, which took seven days to arrive. Plaintiff Brulinski had no convenient way to access his bank account funds in the meantime. During that time, he could not pay bills or make any withdrawals. He had to visit his bank in-person on two separate occasions to withdraw cash, which was time consuming and inconvenient. Plaintiff Brulinski had never experienced fraudulent charges on his debit card or bank account prior to the Wawa breach. To his knowledge, his debit card number or banking information has not been involved in any other data breaches other than the Wawa breach. Had Mr. Brulinski known that Wawa does not take adequate steps to protect customer Card Information, or had Wawa disclosed to him that it does not, he would not have made purchases at Wawa.

9. Plaintiff Nicole Portnoy is an adult residing in Gaithersburg, Maryland. On Monday, November 25, 2019, Ms. Portnoy made purchases at her local Wawa in Maryland, using her Police and Fire Federal Credit Union card ("PFFCU Card"). The next morning, Tuesday,

November 26, 2019, Ms. Portnoy's PFFCU Card that she used to make purchases at Wawa the day before experienced two fraudulent charges totaling $1,200: one on HP's online store in excess of $1,000, and another at Bed Bath & Beyond's retail store in Totowa, New Jersey, in the amount of approximately $100. Ms. Portnoy visited her local bank branch the next day, on November 27, 2019, to dispute the charges, and the bank canceled her card and gave her a replacement card that same day. Ms. Portnoy suffered immense frustration, aggravation and loss of time traveling from her home in Maryland to her bank in Pennsylvania, discussing this situation with her bank, disputing the fraudulent charges, and changing her card information with every vendor that automatically deducts bills and expenses from her account on a recurring basis. Furthermore, the amount of the fraudulent charges exceeded the balance of funds she had in her checking account, so it then automatically pulled the balance of the fraudulent charges from her savings account. Ms. Portnoy experienced additional frustration and loss of time undoing these automatic transfers that resulted proximately and directly from the fraudulent charge.

10. Plaintiff Charmissha Tingle is an adult residing in Wilmington, Delaware. Ms. Tingle used her Rush Debit card for her MetaBank checking account ("Rush Card") at Wawa locations in Delaware during the Data Breach window. On October 15, 2019, Ms. Tingle's Rush Card experienced four separate fraudulent charges on the same day at various locations in California: three restaurants in the amounts of: $50.38, $61.90, $46.25, and an animal hospital in the amount of $178.55. On October 16, 2019, Ms. Tingle contacted MetaBank about the fraudulent charges, and MetaBank reissued her a new card, but did not reverse the charges for two full weeks, on October 29, 2019. During those two weeks, Ms. Tingle was without the funds used to commit the fraudulent charges. As a result of these fraudulent charges, Ms. Tingle ceased using her Rush Card and MetaBank checking account on October 29, 2019. MetaBank charges Ms. Tingle a $5.00

monthly fee for using her account. As of October 29, 2019, Ms. Tingle ceased using her MetaBank account, but was charged the $5.00 monthly fee on November 1, 2019, for the month of November. Thus, as a direct and proximate result of the breach, Ms. Tingle lost the benefits she was due to receive in exchange for paying MetaBank's $5.00 monthly fee for a portion of October and all of November 2019 that she did not use her MetaBank account. After learning about the Wawa Data Breach in December 2019, Ms. Tingle reviewed these four fraudulent charges on her Rush Card/MetaBank statement and realized that she had made purchases at Wawa using her Rush Card only two days before the fraudulent charges. Prior to these fraudulent charges, Ms. Tingle had never previously experienced fraudulent charges on her Rush Card/MetaBank account.

11. Plaintiff April Pierce is a resident of Delaware. She used her debit card on numerous occasions at one or more Wawa locations in Delaware and Pennsylvania during the breach period. After using her debit card at Wawa, she was notified of one attempted fraudulent purchase on the same card. On or around May 15, 2019, she received a call from her bank, Discover Bank, notifying her of suspected fraudulent activity. The bank referenced a charge at a gas station in Lithonia, Georgia. When Plaintiff Pierce went to use her debit card on that same day, it was declined due to the incident in Georgia. She disputed the charge with her bank. The dispute process was time-consuming and involved multiple phone calls with the bank. The bank cancelled her debit card and issued a replacement card, which took 3-5 days to arrive. Plaintiff Pierce had no convenient way to access her bank account funds in the meantime. During that time, she could not pay bills or make any withdrawals. While on the phone with her bank, she had to visit a specific/particular ATM to withdraw cash so that she had a way to pay for things in the following days, which was time consuming and inconvenient. During this time, her bank was able to unfreeze her card for a few minutes to allow her to withdraw cash, and then re-freeze the card

after the ATM transaction was complete. This cash had to hold her over for the 3-5 days until her new debit card arrived and if she ran out of cash, she had no reasonable means to withdraw additional cash. Plaintiff Pierce had never experienced any fraudulent charges on her debit card or bank account prior to the Wawa breach. To her knowledge, her debit card number or banking information has not been involved in any other data breaches other than the Wawa breach.

12. Plaintiff Kelly Donnelly Bruno is an adult residing in Middlesex, New Jersey. Ms. Donnelly Bruno used her Wells Fargo debit card at affected Wawa locations during the Data Breach window. On December 27, 2019, Ms. Donnelly Bruno discovered fraudulent charges on her Wells Fargo debit card statement. She immediately called Wells Fargo to alert them of the fraud. As a result, Wells Fargo cancelled her debit card. Ms. Donnelly Bruno was without the use of her debit card for 5-10 days, while a new card was being issued. She has spent approximately one hour addressing the fraud she experienced. Prior to being victimized by the Wawa Data Breach, Ms. Donnelly Bruno's Wells Fargo debit card had never been subjected to theft or fraud. Had Ms. Donnelly Bruno known that Wawa would not adequately protect her Card Information and other sensitive information entrusted to it, she would not have made regular purchases at Wawa using her payment card. As a result of Wawa's failure to adequately safeguard Plaintiff Donnelly Bruno's Card Information, she has been injured.

13. Plaintiff Tracey Lucas is an adult residing in Washington, DC. Ms. Lucas used her debit card at affected Wawa locations during the Data Breach window. On or around July 13, 2019, Ms. Lucas noticed possible fraudulent activity on her bank account, including a $400 charge for T-Mobile along with several other fraudulent charges. She reached out to Navy Federal Credit Union to inquire about the possible fraudulent activity she had detected. In response, Navy Federal canceled her existing debit card and closed her account. The fraudulent charges she incurred were

reversed and Ms. Lucas was issued a new debit card for a new account. Ms. Lucas has spent approximately 48 hours addressing the fraud she experienced. Prior to being victimized by the Wawa Data Breach, Ms. Lucas's debit card had never been subjected to theft or fraud. Had Ms. Lucas known that Wawa would not adequately protect her Card Information and other sensitive information entrusted to it, she would not have made regular purchases at Wawa using her payment card. As a result of Wawa's failure to adequately safeguard Plaintiff Lucas's Card Information, she has been injured.

B. Defendant

14. Defendant Wawa, Inc. is a privately held company with its principal place of business in Wawa, Pennsylvania. It is incorporated in New Jersey. It operates 850 convenience stores in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. It employs over 35,000 individuals and with annual revenue over $10 billion, it is one of the largest privately-owned companies in the United States.

III. JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5 million, and many members of the class are citizens of states different from Defendant.

16. This Court has personal jurisdiction over Defendant because Defendant conducts business in and throughout Pennsylvania, and the wrongful acts alleged in the Complaint were committed largely in Pennsylvania.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(1) because Defendant is headquartered in this District

and is a resident for venue purposes because it regularly transacts business here. Further, venue is proper under 28 U.S.C. § 1391(b)(3) because Defendant is subject to personal jurisdiction in this District.

IV. FACTUAL ALLEGATIONS

18. Wawa is an operator of a large chain of convenience stores and gas stations.

19. On December 19, 2019, Defendant publicly announced the Data Breach, stating the following on its website:

> Wawa has experienced a data security incident. Our information security team discovered malware on Wawa payment processing servers on December 10, 2019, and contained it by December 12, 2019. This malware affected customer payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained. . . .
>
> ***
>
> Based on our investigation to date, we understand that at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. Although the dates may vary and some Wawa locations may not have been affected at all, this malware was present on most store systems by approximately April 22, 2019. Our information security team identified this malware on December 10, 2019, and by December 12, 2019, they had blocked and contained this malware. . . .
>
> Based on our investigation to date, this malware affected payment card information, including **credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers beginning at different points in time after March 4, 2019 and ending on December 12, 2019**. Most locations were affected as of April 22, 2019, however, some locations may not have been affected at all. No other personal information was accessed by this malware. . . .[1]

20. Defendant also noted that the malware "may have captured some information about Wawa gift card numbers."[2]

---

[1] https://www.wawa.com/alerts/data-security, Notice tab (emphasis added) (last visited Dec. 21, 2019).

[2] https://www.wawa.com/alerts/data-security, Frequently Asked Questions tab (last visited Dec. 21, 2019).

21. Defendant disclosed that CVV2 numbers (the three or four-digit security code printed on the back of credit and debit cards) were not stolen in the breach.[3] However, thieves reportedly can still make fraudulent purchases without access to the security code:

> [T]hree- or four-digit security codes weren't stolen, but that doesn't necessarily matter for the hackers, per [data security expert Matthew] Wilson. A three-digit code has only 999 possible answers, after all. "That sounds like lot to human," he says. "To a machine, it's nothing."[4]

22. Defendant failed to properly safeguard class members' Card Information, allowing cybercriminals to access credit and debit Card Information for many months undetected. Defendant also failed to properly monitor its systems. Had it properly monitored its card payment systems, it would have discovered the malware much sooner than nine months after the breach began.

23. Defendant had a duty pursuant to common law, industry standards, card network rules, and representations made in its own privacy policy to keep consumers' Card Information confidential and to protect it from unauthorized access.

24. The Pennsylvania Attorney General has initiated an investigation into Wawa's role in the Data Breach.[5]

A. Wawa Was on Notice of a Significant Risk of a Data Breach

25. Defendant's data security obligations were particularly important and well-known to Defendant given the substantial increase in payment card data breaches throughout the retail industry preceding the Data Breach, including numerous recent malware-based payment card

---

[3] https://www.wawa.com/alerts/data-security, Notice tab (last visited Dec. 21, 2019).
[4] *The Wawa Credit Card Breach: What You Need to Know*, Philadelphia Magazine, Dec. 20, 2019, *available at* https://www.phillymag.com/news/2019/12/20/wawa-data-breach/ (last visited Jan. 9, 2020).
[5] https://www.law360.com/retail/articles/1230186/wawa-data-breach-exposed-credit-debit-card-numbers (last visited Jan. 9, 2020).

breaches. The increase in data breaches, and the risk of future breaches, was widely known throughout the retail industry, including to Defendant.

26. Indeed, during the period of the Data Breach, Visa warned gas station operators about an increase in hackers targeting internal payment processing systems at gas stations. The warning specified that hackers have been targeting internal processing systems, not just external card-swipe terminals attached to gas pumps.

27. Specifically, Visa distributed a "Security Alert" dated November 2019 stating the following, in relevant part:

> In August and September 2019, Visa Payment Fraud Disruption (PFD) investigated two separate breaches at North American fuel dispenser merchants. The attacks involved the use of point-of-sale (POS) malware to harvest payment card data from fuel dispenser merchant POS systems. It is important to note that **this attack vector differs significantly from skimming at fuel pumps, as the targeting of POS systems requires the threat actors to access the merchant's internal network**. In one of the two cases investigated by PFD, the threat actors successfully compromised the merchant's network through a phishing email that contained a malicious attachment. Once the malware was deployed on the merchant's network, it scraped Track 1 and Track 2 payment card data from the random access memory (RAM) of the targeted POS system. The threat actors were able to obtain this payment card data due to the lack of secure acceptance technology, (e.g. EMV® Chip, Point-to-Point Encryption, Tokenization, etc.) and non-compliance with PCI DSS.
>
> **The targeting of fuel dispenser merchants is the result of the slower migration to chip technology on many terminals, which makes these merchants an attractive target for criminal threat actors attempting to compromise POS systems for magnetic stripe payment card data**.
>
> . . . .
>
> The recent attacks are attributed to two sophisticated criminal groups with a history of large-scale, successful compromises against merchants in various industries. The groups gain access to the targeted merchant's network, move laterally within the network using malware toolsets, and ultimately target the merchant's POS environment to scrape payment card data. The groups also have close ties with the cybercrime underground and are able to easily monetize the accounts obtained in these attacks by selling the accounts to the top tier cybercrime underground carding shops.

> Fuel dispenser merchants should take note of this activity as the group's operations are significantly more advanced than fuel dispenser skimming, and these attacks have the potential to compromise a high volume of payment accounts. The deployment of devices that support chip will significantly lower the likelihood of these attacks.[6]

28. The Visa warning specified that hackers were placing "malware" onto card processing systems. Notably, the Wawa Data Breach involved malware.

29. The Visa warning also specified that hackers were attacking gas station merchants that had not yet upgraded to chip technology. Notably, Wawa had not yet fully upgraded to chip technology at the time of the Data Breach.[7]

30. One particular data security expert noted that the Wawa Data Breach may have resulted from an employee clicking on a phishing link, which was the precise risk flagged by the Visa alert:

> Michael Levy, former chief of computer crimes at the U.S. Attorney's Office for the Eastern District of Pennsylvania, wrote in an email[:] . . . "[I]f you can get an employee inside the company to click on a link, and that link causes the employee's computer to download malware, you have tunneled under the moat and [fire]wall. It was my guess that the perpetrators accomplished the Wawa breach in a similar fashion."[8]

31. The Visa warning highlighted specific risks factors that were present within Wawa's payment card and computer systems, and warned of the precise type of hacking that

---

[6] Visa Security Alert (November 2019), *available at* https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf (last visited Jan. 9, 2020) (emphasis added).

[7] *Before Wawa Found Data Breach Exposing Customers' Credit and Debit Cards, Visa Warned It Could Happen*, Philadelphia Inquirer (Jan. 2, 2020), *available at* https://www.inquirer.com/business/wawa-visa-hacks-identity-theft-suits-20200102.html ("Wawa said this week that it is implementing chip technology at gas pumps and expects all pumps to be upgraded in 2020.").

[8] *Before Wawa Found Data Breach Exposing Customers' Credit and Debit Cards, Visa Warned It Could Happen*, Philadelphia Inquirer (Jan. 2, 2020), *available at* https://www.inquirer.com/business/wawa-visa-hacks-identity-theft-suits-20200102.html (last visited Jan. 9, 2020).

ultimately took place at Wawa. The Visa warning placed Wawa on further notice of an unusually high risk of a data breach. Wawa failed to improve its cardholder data security despite these known critical risks.

B. Wawa Has a History of Credit Card Data Breaches

32. Wawa has a history of credit card intrusions.

33. In 2013, Wawa customers suffered credit card fraud tied to the theft of card information from one of its convenience stores:

> Customers who shopped at a Wawa on Salem Road in Burlington, New Jersey noticed fraudulent purchases on their credit cards. Investigators were able to trace the fraud to four people and arrest them. The four men were charged with credit card theft, credit card fraud, identity theft, and having electronic devices for criminal use. More victims are expected to be found.[9]

34. Similarly, in 2018, police investigated a skimming device placed on a Wawa gas pump, which reportedly led to fraudulent credit card purchases.[10]

35. These breaches, coupled with numerous others impacting other retail companies, put Defendant on notice of the importance of data security, the fact that thieves were aggressively seeking stolen credit card information from Wawa, and the harm that could result from weak data security. Despite these events, Defendant nevertheless failed to adopt adequate data security governing its credit and debit card transactions.

C. Defendant's Privacy Policy

36. Defendant's Privacy Policy stated that data security is important to Wawa and that Wawa is committed to safeguarding consumer data:

---

[9] https://privacyrights.org/data-breaches (Excel spreadsheet describing data breaches) (last visited Jan. 9, 2020).

[10] *Police Investigating Credit Fraud Related to Wawa*, Northeast Times, May 24, 2018, *available at* https://northeasttimes.com/2018/05/24/police-investigating-credit-fraud-related-to-wawa/ (last visited Jan. 9, 2020).

> Protecting your privacy is important to Wawa. This Wawa Privacy Policy ("Policy") describes how Wawa and its subsidiaries and affiliated companies collect, use, disclose and safeguard the personal information . . . collected when you visit our stores or otherwise communicate or interact with Wawa.
>
> . . . .
>
> We may collect any information, such as your first and last name, credit card number, email address, postal address, and telephone number that you provide when you interact with Wawa. Some examples are when you: Make an online or in-store purchase. . . .
>
> . . . .
>
> Data Security
>
> Wawa is fully committed to data security.[11]

37. Plaintiffs and class members provided their Card Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep the card information confidential and would secure it from unauthorized access. Defendant failed to do so, in contravention of its own privacy policy.

D. Defendant's Data Security Failures

38. Defendant breached its duties, obligations, and promises by not:

a. Adequately safeguarding consumers' Card Information;

b. Maintaining an adequate data security environment to reduce the risk of a data breach;

c. Properly monitoring its data security systems for existing intrusions and weaknesses;

d. Performing penetration tests to determine the strength of its payment card processing systems;

[11] https://www.wawa.com/privacy (last visited Dec. 21, 2019).

e. Properly training its information technology staff on matters relevant to cardholder data security; and

f. Retaining outside vendors to periodically test its payment card processing systems.

39. With respect to Wawa's monitoring procedures, industry experts have acknowledged that the lengthy period of the Data Breach is indicative of Wawa's faulty monitoring systems:

> "What is most shocking to me, and should be most appalling to everybody, is how long this went undetected. How did Wawa just find this recently?" said Ron Schlecht, managing partner at Bala Cynwyd-based BTB Security. "They were obviously not monitoring at an appropriate level commensurate with their business volume and were unable to detect this anomalous activity."[12]

1. Defendant Violated PCI Data Security Standards

40. There is an extensive network of financial institutions, card-issuing banks, and card-processing companies involved in credit and debit card transactions. Card networks have issued detailed rules and standards governing the basic protective measures that merchants like Wawa must take to ensure that payment card information is properly safeguarded.

41. The payment card networks (primarily MasterCard, Visa, American Express, and Discover) have issued card operating rules that are binding on merchants including Defendant and require merchants to protect cardholder data. In particular, the Payment Card Industry Security Standards Council promulgates minimum standards that apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry

[12] *Before Wawa Found Data Breach Exposing Customers' Credit and Debit Cards, Visa Warned It Could Happen*, Philadelphia Inquirer (Jan. 2, 2020), *available at* https://www.inquirer.com/business/wawa-visa-hacks-identity-theft-suits-20200102.html (last visited Jan. 9, 2020).

Data Security Standards ("PCI DSS"). PCI DSS is the industry standard governing the security of credit and debit card data.

42. PCI DSS establishes detailed comprehensive requirements for satisfying each of the following twelve "high-level" mandates:[13]

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

43. As noted in the chart, PCI DSS required Defendant to "protect all systems against malware." Defendant failed to do so. Defendant specified that the hacker(s) placed "malware" on Defendant's payment processing servers.

44. PCI DSS also required Defendant to "[t]rack and monitor all access to network resources." Defendant failed to do so. The hacker(s) had access to Defendant's system for nine months, illustrating that Defendant had materially deficient tracking and monitoring systems in place.

[13] *Payment Card Industry (PCI) Data Security Standard*, PCI Security Standards Council, May 2018, at p. 5, *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1577046042482 (last visited Jan. 9, 2020).

45. On information and belief, Defendant violated numerous other provisions of the PCI DSS, including subsections underlying the chart above. Those deficiencies will be revealed during discovery with the assistance of expert witnesses.

46. PCI DSS sets the minimum level of what must be done, not the maximum. While PCI compliance is an important first step in securing cardholder data, it is not sufficient on its own to protect against all breaches, nor does it provide a safe harbor against civil liability for a data breach.

47. At all relevant times, Defendant was well-aware of its PCI DSS obligations to protect cardholder data. Defendant was an active participant in the payment card networks as it collected and transmitted millions of sets of payment card data per day.

48. Industry experts acknowledge that a data breach is indicative of data security failures. For example, research and advisory firm Aite Group has stated: "'If your data was stolen through a data breach that means you were somewhere out of compliance' with payment industry data security standards."[14]

2. Defendant Violated the FTC Act

49. The Federal Trade Commission ("FTC") has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §45.

50. The FTC published guidance establishing reasonable data security practices for businesses. The FTC guidance notes that businesses should, e.g.: protect the personal customer

[14] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), *available at* http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last accessed Jan. 9, 2020).

information that they acquire; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security vulnerabilities. FTC guidance also recommends that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and watch for large amounts of data being transmitted from the system.[15]

51. The FTC has issued orders against businesses for failing to employ reasonable measures to safeguard customer data. The orders provide further public guidance to businesses concerning their data security obligations.

52. Defendant knew or should have known about its obligation to comply with the FTC Act regarding data security.

53. Defendant's misconduct violated the FTC Act, led to the Data Breach, and caused harm to Plaintiffs and class members.

E. Misuse of the Stolen Data Has Begun

54. Widespread misuse of the stolen cardholder data has already begun.

55. Plaintiffs have suffered fraudulent charges on their payment cards, as discussed in detail above.

56. Similarly, plaintiffs in numerous other Class Action Complaints filed against Wawa have specified that they suffered fraudulent charges on the credit and debit cards they used at Wawa.

---

[15] *See, e.g.*, *Start with Security: A Guide for Business*, Federal Trade Commission, June 2015, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, Oct. 2016, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

57. Visa and MasterCard have issued Compromised Account Management System ("CAMS") alerts to card-issuing banks to highlight the risk of fraud on the banks' specific payment cards used at Wawa during the Data Breach period.[16]

58. In reaction to the risk of fraudulent purchases, some card-issuing banks have begun issuing replacement cards to thousands of customers who used their payment cards at Wawa during the period of the Data Breach.[17] Given the significant cost of issuing replacement cards, banks do not routinely issue replacement cards unless the risk of fraud is particularly high in light of known fraudulent activity.

F. Damages to Class Members

59. The Data Breach is particularly egregious and Wawa's data security failures are particularly alarming given that the breach reportedly lasted nine months and impacted all of Wawa's 850+ locations. Each Plaintiff and the class members have been damaged by the compromise of their Card Information in the Data Breach.

60. Class members also face a substantial and imminent risk of fraudulent charges on their payment cards. Criminals carried out the Data Breach and stole the Card Information with the intent to use it for fraudulent purposes and/or to sell it.

61. Plaintiffs and class members have already experienced fraudulent credit and debit card purchases, and other class members will experience fraud going forward.

---

[16] See *First Choice Federal Credit Union v. Wawa, Inc. and Wild Goose Holding Co., Inc.*, Case No. 2:20-cv-00011 (W.D. Pa.), Class Action Complaint at ¶ 31 ("Beginning on Friday, December 27, 2019, Visa issued a series of Compromised Account Management System ('CAMS') alerts to Plaintiff, indicating that the estimated fraud 'exposure window' for the WaWa Data Breach ran from April 22, 2019 through December 13, 2019. . . . According to the CAMS alerts received by Plaintiff, at least 65 payment cards issued by Plaintiff to its members were compromised as a result of the WaWa Data Breach.").

[17] *After Wawa Breach, Banks Reissue Thousands of Debit, Credit Cards to Customers*, Philadelphia Inquirer (Jan. 3, 2020), available at https://www.inquirer.com/news/wawa-citibank-citizens-bank-credit-debit-breach-hack-20200103.html.

62. Also, many class members will incur out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

63. Class members also suffered a "loss of value" of their credit and debit card information when it was stolen by the hacker in the Data Breach. A robust market exists for stolen card information, which is sold on the dark web at specific identifiable prices. This market serves as a means to determine the loss of value to class members.

64. Class members also suffered "benefit of the bargain" damages. Class members overpaid for goods that should have been – but were not – accompanied by adequate data security. Part of the price class members paid to Defendant was intended to be used to fund adequate data security. Class members did not get what they paid for.

65. Class members have spent and will continue to spend substantial amounts of time monitoring their payment card accounts for fraud, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. Class members will also spend time obtaining replacement cards and resetting automatic payment links to their new cards. These efforts are burdensome and time-consuming.

66. Class members who experience actual fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to the fraudulent charges. Class members will also be harmed by the loss of use of and access to their account funds and credit lines, or being limited in the amount of money they are permitted to obtain from their accounts. Class members will further be harmed by the loss of rewards points or airline mileage available on credit cards that consumers lost credit for as a result of having to use alternative forms of payment while awaiting replacement cards. This includes missed

payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

67. The stolen Card Information is a valuable commodity to identity thieves. Upon information and belief, many millions of sets of customer Card Information were stolen and illegally placed for sale on the "dark web"—an underground or "black market" part of the internet accessed by an anonymizing browser and that is not indexed by search engines, where rampant illegal commerce occurs (*e.g.*, buying and selling stolen card, subscription, and account information/credentials; buying and selling drugs, guns, and counterfeit money). The purpose of stealing large caches of Card Information is to use it to defraud consumers or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit payment card fraud. One commentator discussing the Wawa breach noted that "the nature of the burgled items [at Wawa] makes it a foregone conclusion that they will be peddled on the dark web."[18]

68. Cyber criminals routinely post stolen payment card information on anonymous websites, making the information widely available to a criminal underworld. There is an active and robust market for this information.

69. The risk of fraud will persist for years. Identity thieves often hold stolen data for months or years before using it, to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer.

70. Thus, class members must vigilantly monitor their financial accounts for months or years to come.

---

[18] *Wawa Data Breach: Security Incident Details and Updates* (Dec. 22, 2019), *available at* https://www.msspalert.com/cybersecurity-breaches-and-attacks/wawa-security-incident-details/ (last visited Jan. 14, 2020).

1. Class Members Face a Risk of Identity Theft Beyond Just Credit and Debit Card Fraud

71. Identity thieves can combine data stolen in the Data Breach with other information about class members gathered from underground sources, public sources, or even class members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to class members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes including, e.g., opening new financial accounts in class members' names, taking out loans in class members' names, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names but with another person's photograph, and giving false information to police during an arrest.

72. Defendant has acknowledged that class members face a significant risk of various types of identity theft stemming from the Data Breach. Shifting the burden of responding to the Data Breach to consumers, Defendant recommended that affected customers undertake the following errands: (i) review their credit and debit card statements carefully to identity fraudulent transactions; (ii) obtain a copy of their credit report to "look for any inaccuracies and/or accounts you don't recognize"; (iii) place a "fraud alert" on their credit file to "protect you against the possibility of an identity thief opening new credit accounts in your name"; and (iv) place a "security freeze" on their credit file to prevent creditors from accessing the credit file without the consumer's consent.[19] Thus, Defendant acknowledges that class members face a risk of identity theft beyond just fraudulent credit and debit card transactions.

73. To protect against these broad-based types of fraud, Defendant has offered only one year of free credit monitoring and identity theft insurance to all customers whose card information

[19] https://www.wawa.com/alerts/data-security, "Notice" tab (last visited Dec. 21, 2019).

was stolen in the Data Breach, at the credit monitoring service of Defendant's choice. This limited offering of protection is insufficient to combat the indefinite risk of fraud beyond one year. Furthermore, this type of protection would not have been necessary if consumers' risk was limited to just fraudulent credit and debit card transactions.

V. CLASS ACTION ALLEGATIONS

74. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a Nationwide Class. In the alternative, Plaintiffs bring this case on behalf of the following state classes as defined below: a Pennsylvania Class, a Florida Class, a Maryland Class, a Delaware Class, a New Jersey Class, and a Washington, D.C. Class (collectively, the "Classes"), defined as follows:

> Nationwide Class: All persons in the United States whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.
>
> Pennsylvania Class: All residents of the commonwealth of Pennsylvania whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.
>
> Florida Class: All residents of the state of Florida whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.
>
> Maryland Class: All residents of the state of Maryland whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.
>
> Delaware Class: All residents of the state of Delaware whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.
>
> New Jersey Class: All residents of the state of New Jersey whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.
>
> Washington, D.C. Class: All residents of Washington, D.C. whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.

75. Excluded from Classes are Defendant's executive officers, and the judge to whom this case is assigned.

76. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Nationwide Class consists of millions of individuals, and the Pennsylvania, Florida, Delaware, New Jersey, Washington D.C. and Maryland Class each consist of tens of thousands or more individuals. These estimates are based on the fact that the Data Breach affected all or most of Defendant's 850 convenience store locations for a nine-month period.

77. Commonality. There are many questions of law and/or fact common to Plaintiffs and the Classes. Common questions include, but are not limited to, the following:

a. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws, regulations, industry standards, and PCI DSS requirements;

b. Whether Defendant owed a duty to class members to safeguard their payment card information;

c. Whether Defendant breached its duty to class members to safeguard their payment card information;

d. Whether a computer hacker obtained class members' payment card information in the Data Breach;

e. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

f. Whether Plaintiffs and class members suffered legally cognizable damages as a result of the Data Breach; and

g. Whether Plaintiffs and class members are entitled to injunctive relief.

78. Typicality. Plaintiffs' claims are typical of the claims of all class members because Plaintiffs, like other class members, suffered a theft of their cardholder information in the Data Breach.

79. Adequacy of Representation. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs have retained competent and capable counsel with significant experience in complex class action litigation, including data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Classes. Plaintiffs' counsel has the financial and personnel resources to do so. Neither Plaintiffs nor their counsel have interests that are contrary to, or that conflict with, those of the Classes.

80. Predominance. Defendant has engaged in a common course of conduct toward all class members. The common issues arising from Defendant's conduct predominate over any issues affecting just individual class members. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

81. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would find that the cost of litigating their individual claim is prohibitively high, and they would have no effective remedy on an individual non-class basis. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to class members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action on a class-wide basis presents far fewer

management difficulties, conserves judicial resources and the parties' resources, and protects the rights of all class members.

82. Defendant has acted on grounds that apply generally to the Classes as a whole, so that injunctive relief is appropriate on a class-wide basis pursuant to Fed. R. Civ. P. 23(b)(2).

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of Plaintiffs, the Nationwide Class, and, in the alternative, all State Classes)

83. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

84. Defendant obtained class members' credit and debit card information in connection with class members' purchases at Defendant's stores.

85. By collecting and maintaining cardholder data, Defendant had a duty of care to use reasonable means to secure and safeguard the cardholder information and to prevent disclosure of the information to unauthorized individuals. Defendant's duty included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

86. Defendant owed a duty of care to Plaintiffs and class members to provide data security consistent with the various requirements and rules discussed above.

87. Defendant's duty of care arose as a result of, among other things, the special relationship that existed between Defendant and its customers. Defendant was in position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur, which would result in substantial harm to consumers. Indeed, Defendant's announcement

of the Data Breach acknowledged that Defendant was in a "special relationship" with its customers for purposes of protecting their cardholder information.[20]

88. Also, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to use reasonable measures to protect confidential consumer data.

89. Defendant's duty to use reasonable care in protecting cardholder data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards and PCI DSS rules to protect cardholder information.

90. Defendant was subject to an "independent duty" untethered to any contract between class members and Defendant.

91. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect cardholder information. Defendant's negligent acts and omissions include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard cardholder information;

b. Failing to adequately monitor the security of Defendant's payment card processing network;

c. Allowing unauthorized access to class members' sensitive cardholder information;

d. Failing to detect in a timely manner that class members' cardholder information had been compromised; and

[20] https://www.wawa.com/alerts/data-security, Notice tab (last visited Dec. 21, 2019).

e. Failing to timely notify class members about the Data Breach so that they could take appropriate steps to mitigate the risk of identity theft and other damages.

92. It was foreseeable to Defendant that a failure to use reasonable measures to protect cardholder information could result in injury to consumers. Further, actual and attempted breaches of data security were reasonably foreseeable to Defendant given the known frequency of payment card data breaches: (i) in the retail industry in general, (ii) at gas stations in particular, and (iii) at Defendant's operations specifically.

93. Plaintiffs and class members suffered various types of damages as alleged above.

94. Defendant's wrongful conduct was a proximate cause of class members' damages.

95. Plaintiffs and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

96. Plaintiffs and class members are also entitled to injunctive relief requiring Defendant to, e.g.,: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all class members.

COUNT II

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs, the Nationwide Class, and, in the alternative, all State Classes)

97. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

98. When Plaintiffs and class members provided their card information to Defendant in exchange for Defendant's products, they entered into implied contracts with Defendant under which Defendant agreed to take reasonable steps to protect the card information.

99. Defendant solicited and invited class members to provide their card information as part of Defendant's regular business practices. Plaintiffs and class members accepted Defendant's offers and provided their card information to Defendant.

100. When entering into the implied contracts, Plaintiffs and class members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

101. Defendant's implied promise to safeguard cardholder information is evidenced by, e.g., the representations in Defendant's Privacy Policy set forth above.

102. Plaintiffs and class members paid money to Defendant to purchase items at Defendant's convenience stores. Plaintiffs and class members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

103. Plaintiffs and class members would not have provided their card information to Defendant in the absence of Defendant's implied promise to keep the card information reasonably secure.

104. Plaintiffs and class members fully performed their obligations under the implied contracts by paying money to Defendant.

105. Defendant breached its implied contracts with Plaintiffs and class members by failing to implement reasonable data security measures.

106. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and class members sustained damages as alleged herein.

107. Plaintiffs and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

108. Plaintiffs and class members are also entitled to injunctive relief requiring Defendant to, e.g.: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all class members.

COUNT III

VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Stat. §§ 201-1 to 201-9.2 ("UTPCPL") (On Behalf of Plaintiffs and the Pennsylvania Class)

109. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

110. Plaintiffs and Defendant are each a "person" as defined at 73 Pa. Stat. § 201-2(2).

111. Plaintiffs and Pennsylvania Class members purchased goods and services in "trade" and "commerce" as defined at 73 Pa. Stat. § 201-2(3).

112. Plaintiffs and Pennsylvania Class members purchased goods and services primarily for personal, family, and/or household purposes under 73 Pa. Stat. § 201-9.2.

113. Defendant engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined at 73 Pa. Stat. § 201-2(4) by engaging in the following conduct:

a. Representing that its goods and services had characteristics, uses, benefits, and qualities that they did not have – namely that its goods, services, and business practices were accompanied by adequate data security (73 Pa. Stat. § 201-2(4)(v));

b. Representing that its goods and services were of a particular standard or quality when they were of another quality (73 Pa. Stat. § 201-2(4)(vii));

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. § 201-2(4)(ix); and

d. "Engaging in any other . . . deceptive conduct which creates a likelihood of confusion or of misunderstanding" (73 Pa. Stat. § 201-2(4)(xxi)).

114. These unfair methods of competition and unfair or deceptive acts or practices are declared unlawful by 73 Pa. Stat. § 201-3.

115. Defendant's unfair or deceptive acts and practices include but are not limited to: failing to implement and maintain reasonable data security measures to protect cardholder information; failing to identify foreseeable data security risks and remediate the identified risks; failing to comply with common law duties, industry standards including PCI DSS, and FTC guidance regarding data security; misrepresenting in its Privacy Policy that it would protect cardholder data; and omitting and concealing the material fact that it did not have reasonable measures in place to safeguard cardholder data.

116. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security practices and ability to protect cardholder information.

117. Defendant intended to mislead consumers and induce them to rely on its misrepresentations and omissions. As set forth herein, Plaintiffs did rely on Defendant's misrepresentations and omissions relating to its data privacy and security.

118. Plaintiffs and Pennsylvania Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

119. Had Defendant disclosed to consumers that its data security systems were not secure and, thus, were vulnerable to attack, Plaintiffs and class members would not have given their payment data to Defendant.

120. Defendant acted intentionally, knowingly, and maliciously in violating the Pennsylvania UTPCPL, and recklessly disregarded consumers' rights.

121. Defendant's past payment card data breaches put it on notice of the importance of data security and that its card processing system was subject to attack.

122. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs and Pennsylvania Class members have suffered and will continue to suffer damages, injury, ascertainable losses of money or property, and monetary and non-monetary damages as described above.

123. Plaintiffs and Pennsylvania Class members seek all monetary and non-monetary relief allowed by law, including the following as expressly permitted under 73 Pa. Stat. § 201-9.2:

a. "actual damages or [statutory damages of] one hundred dollars ($100), whichever is greater";

b. treble damages, defied as "three times the actual damages";

c. "reasonable attorney fees" and litigation costs; and

d. "such additional relief as [the Court] deems necessary or proper."

124. Plaintiffs and Pennsylvania Class members also seek the injunctive relief as set forth above.

COUNT IV

VIOLATIONS OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. § 501, *et seq*. ("FDUTPA")
(On Behalf of Plaintiff McDaniel and the Florida Class)

125. Plaintiff McDaniel re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

126. Plaintiff McDaniel and members of the Florida Class are "consumers" for purposes of Fla. Stat. § 501.203(7).

127. Plaintiff McDaniel and members of the Florida Class purchased "things of value" in the form of their goods and services acquired from Defendant. These purchases were made for personal, family, or household purposes. Fla. Stat. § 501.203(9).

128. Defendant engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale of goods or services to consumers, including to members of the Florida Class. Fla. Stat.§ 501.203(8).

129. Defendant engaged in, and its acts and omissions affected, trade and commerce.

130. Defendant's acts, practices, and omissions were done in the course of Defendant's business of advertising, marketing, offering to sell, and selling goods and services throughout Florida and the United States. Fla. Stat. § 501.203(8).

131. Defendant, operating in Florida, engaged in deceptive, unfair, and unlawful acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. Representing that it maintained (when it failed to maintain) adequate data security practices to safeguard cardholder data;

b. Representing that its data security practices were adequate, while failing to disclose that its data security practices were inadequate to safeguard cardholder data from theft; and

c. Failing to timely and accurately disclose the Data Breach to class members.

132. This conduct is considered an unfair method of competition, and constitutes unfair and unconscionable acts and practices. Fla. Stat. § 501.204(l).

133. As a direct and proximate result of Defendant's violation of the FDUTPA, Plaintiff McDaniel and members of the Florida Class suffered actual damages by paying a premium for Defendant's goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate data security practices that comply with industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices. Fla. Stat. § 501.211(2).

134. Also, as a direct result of Defendant's knowing violation of the FDUTPA, Plaintiff McDaniel and members of the Florida Class are not only entitled to actual damages, but also a declaratory judgment stating that Defendant's actions and practices alleged herein violate the FDUTPA.

135. Plaintiff McDaniel and members of the Florida Class are also entitled to injunctive relief requiring Defendant to, e.g.: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all class members. Fla. Stat. § 501.211(1).

136. Plaintiff McDaniel brings this action on behalf of himself and members of the Florida Class for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect consumers from Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices.

137. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

138. The above unfair and deceptive practices and acts by Defendant were unmoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff

McDaniel and members of the Florida Class that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

139. Defendant knew or should have known that its data security practices were inadequate to safeguard consumers' cardholder information, and that the risk of a data theft was high.

140. Defendant's actions and inactions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

141. Plaintiff McDaniel and members of the Florida Class seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq*., including, but not limited to, damages, injunctive relief, attorneys' fees and costs, and any other just and proper relief.

COUNT V

VIOLATIONS OF THE MARYLAND CONSUMER PROTECTION ACT
(Md. Code Ann. Com. Law § 13-101, *et seq*.)
(On Behalf Plaintiff Brulinski and the Maryland Class)

142. Plaintiff Brulinski re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

143. Defendant is a "person" as defined by Md. Code Ann. Com. Law § 13-101(h).

144. Defendant's conduct as alleged herein related to "sales" or "offers for sale" as defined by Md. Code Ann. Com. Law § 13-101(i) and § 13-303.

145. Plaintiff Brulinski and members of the Maryland Class are "consumers" as defined by Md. Code Ann. Com. Law § 13-101(c).

146. Defendant advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Code Ann. Com. Law § 13-101(d).

147. Defendant advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting Maryland residents.

148. Defendant engaged in unfair and deceptive trade practices, in violation of Md. Code Ann. Com. Law § 13-301 by, among other things, making false or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers (Md. Code Ann. Com. Law § 13-301(1)); representing that consumer goods or services have a characteristic that they do not have (Md. Code Ann. Com. Law § 13-301(2)(i)); representing that consumer goods or services are of a particular standard, quality, or grade that they are not (Md. Code Ann. Com. Law § 13-301(2)(iv)); failing to state a material fact where the failure deceives or tends to deceive (Md. Code Ann. Com. Law § 13-301(3)); advertising or offering consumer goods or services without intent to sell them as advertised or offered (Md. Code Ann. Com. Law § 13-301(5)); and engaging in deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of a material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services (Md. Code Ann. Com. Law § 13-301(9)).

149. Defendant specifically engaged in unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services, in violation of Md. Code Ann. Com. Law § 13-303 by, among other things, failing to implement and maintain reasonable data security measures to protect consumers' payment card information, which was a direct and proximate cause of the Data Breach; failing to identify foreseeable security and privacy risks; failing to remediate identified security and privacy risks; failing to comply with common law and statutory duties pertaining to the security and privacy of consumers' payment card information, including duties imposed by the FTC Act, 15 U.S.C. § 45; misrepresenting that it would protect

the privacy of consumers' payment card information, including by implementing and maintaining reasonable security measures; omitting, suppressing, and concealing the material fact that it did not adequately secure consumers' payment card information; and omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of consumers' payment card information.

150. Defendant's misrepresentations and omissions were material because they were likely to deceive reasonable consumers (including Plaintiff Brulinski and members of the Maryland Class) about the adequacy of Defendant's data security and ability to protect cardholder information. Defendant's misrepresentations and omissions were important to a significant number of consumers (including Plaintiff Brulinski and members of the Maryland Class) in making decisions to use payment cards as Defendant's convenience stores.

151. Defendant intended to mislead Plaintiff Brulinski and members of the Maryland Class and induce them to rely on its misrepresentations and omissions.

152. Plaintiff Brulinski and members of the Maryland Class acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

153. Defendant acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded the rights of consumers.

154. Defendant's above-described wrongful actions and omissions directly and/or proximately resulted in the various types of harm to Plaintiff Brulinski and members of the Maryland Class identified in detail above.

155. Plaintiff Brulinski and members of the Maryland Class seek all monetary and non-monetary relief allowed by law, including damages, restitution, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT VI

VIOLATIONS OF THE DELAWARE CONSUMER FRAUD ACT
6 Del. Code §§ 2513, *et seq.*
(On Behalf Plaintiff Tingle and the Delaware Class)

156. Plaintiff Tingle re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

157. Wawa is a "person" involved in the "sale" of "merchandise" as each term is defined under 6 Del. Code §§ 2511(6)-(8).

158. Wawa advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware, including Plaintiff.

159. Wawa used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Delaware Class members' Card Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Class members' Card Information, including duties imposed by, *inter alia,* the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Delaware Class members' Card Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Delaware Class members' Card Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100.

160. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Card Information.

161. Defendant acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiff and Delaware Class members' rights. Wawa's past data breaches discussed *supra*, and the multitude of recent, similar malware-based payment card breaches put it on notice that its security and privacy protections were inadequate.

162. Had Defendant disclosed to Plaintiffs and Delaware Class members that its data systems were not secure and, thus, vulnerable to attack, Wawa would have been forced to adopt reasonable data security measures and comply with the law. Instead, it held itself out as a company that values data privacy, and it was entrusted with sensitive and valuable Card Information for millions of consumers, including Plaintiff and the Delaware Class. Plaintiff and the Delaware Class

members acted reasonably in relying on Wawa's misrepresentations and omissions, the truth of which they could not have discovered.

163. Wawa's unlawful trade practices were gross, oppressive, and aggravated, and it breached the trust of Plaintiff and the Delaware Class members.

164. As a direct and proximate result of Wawa's unlawful acts and practices, Plaintiff and Delaware Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; and increased, imminent risk of fraud and identity theft.

165. Plaintiff Tingle and Delaware Class members seek all monetary and nonmonetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Wawa's unlawful conduct; injunctive relief; and reasonable attorneys' fees and costs.

COUNT VII

VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J. Stat. Ann. §§ 56:8-2, *et seq.* ("NJCFA") (On Behalf of Plaintiff Bruno and the New Jersey Class)

166. Plaintiff Bruno re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

167. Plaintiff Bruno and New Jersey Class members are consumers who used their credit or debit cards to purchase convenient store items and gasoline products for personal, family and household purposes from Wawa locations in New Jersey.

168. Wawa engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of "merchandise" to consumers, as defined by N.J. Stat. Ann. § 56:8-1.

169. Wawa is engaged in, and its acts and omissions affect, trade and commerce. Wawa's relevant acts, practices and omissions complained of in this action were done in the course of Wawa's business of marketing, offering for sale and selling food products, gasoline, goods and services throughout the state of New Jersey and the eastern United States.

170. The NJCFA prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New Jersey.

171. In the conduct of its business, trade, and commerce, and in the sale of food products, gasoline, goods or services to consumers in the state of New Jersey, Wawa collected and stored highly personal and private information, including sensitive Card Information of Wawa's customers, like Plaintiff and New Jersey Class members.

172. Wawa knew or should have known that its computer systems and data security practices were inadequate to safeguard class members' sensitive Card Information and that there was a high risk of a data breach.

173. Wawa should have disclosed this information regarding its computer systems and data security practices because Wawa was in a superior position to know the true facts related to the security vulnerability, and members of the class could not reasonably be expected to learn or discover the true facts.

174. As alleged herein, Wawa engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the sale of food products, gasoline products,

goods or services to consumers in the state of New Jersey, in violation of the NJCFA, including but not limited to:

a. Failing to adequate secure the sensitive financial information of members of the New Jersey Class;

b. Failing to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information;

c. Misrepresenting the material fact that Wawa would maintain adequate data privacy and security practices and procedures to safeguard customer's sensitive financial information from unauthorized disclosure, release, data breaches, and theft;

d. Misrepresenting the material fact that Wawa did and would comply with the requirements of relevant federal and state laws and industry standards pertaining to the privacy and security of the sensitive financial information of members of the New Jersey Class;

e. Knowingly omitting, suppressing, and concealing the material fact that Wawa's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, with the intent that others rely upon the omission, suppression, and concealment;

f. Failing to disclose in a timely and accurate manner to the New Jersey Class the material fact of the nature and extent of the Data Breach; and

g. Continuing to accept credit and debit card payments and storage of other personal information after Wawa knew or should have known of the data breach and before it allegedly remedied the breach.

175. By engaging in the conduct alleged above, Wawa has violated the NJCFA by, *inter alia*:

a. Omitting material facts regarding the goods and services sold;

b. Omitting material facts regarding the financial transactions, particularly the security thereof, between Wawa and its customers for the purchase of food products, gasoline, goods and services;

c. Misrepresenting material facts in the furnishing or sale of food products, gasoline, goods and services;

d. Engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

e. Engaging in conduct which creates a likelihood of confusion or of misunderstanding;

f. Engaging in conduct that is immoral, unethical, oppressive and unscrupulous;

g. Unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

h. Other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

176. Wawa's actions engaging in the conduct above were negligent, knowing and willful and/or wanton and reckless with respect to the rights of the Class.

177. As a direct and proximate result of Wawa's violation of the NJCFA, members of the Class have suffered ascertainable losses of moneys and actual damages including, *inter alia*:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information by criminals;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with the unauthorized use of their financial accounts;

e. loss and use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations;

f. costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit monitoring and identity theft protection;

g. impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and already being misused;

h. impairment to their credit scores and ability to borrow and/or obtain credit; and

i. the continued risk to their personal information, which has been accessible to criminals for over nine months and which remains on Wawa's insufficiently secured computer systems.

178. Further, Wawa is a business that compiles or maintains computerized records that include personal information covered under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

179. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business … that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers … of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

180. Because Wawa discovered a breach of its computer systems in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, Wawa had an obligation to disclose the Wawa data breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. § 56:8-163, *et seq.*

181. By failing to disclose the Wawa data breach in a timely and accurate manner, Wawa violated N.J. Stat. Ann. § 56:8-163(b).

182. Pursuant to N.J. Stat. Ann. § 56:8-166, Wawa's violation of N.J. Stat. Ann. § 56:8-153 constitutes a violation of the NJCFA, and is enforceable through N.J. Stat. Ann. § 56:8-19.

183. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Wawa alleged herein, Plaintiff Bruno and New Jersey Class members seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

184. Pursuant to N.J. Stat. Ann. § 56:8-20, this Complaint will be served upon the New Jersey Attorney General.

COUNT VIII

VIOLATION OF THE DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT D.C. Code §§ 28-3901, *et seq.* ("D.C. CPPA") (On Behalf of Plaintiff Lucas and the Washington, D.C. Class)

185. Plaintiff Lucas re-alleges and incorporates by reference all preceding allegations.

186. Wawa is a "person," Plaintiff and Washington, D.C. Class members are "consumers," and Wawa offered for sale "goods and services," as those terms are defined under D.C. CPPA Sections 28-3901(a)(1), (2), and (7).

187. Plaintiff and Washington, D.C. Class members purchased goods and services from Wawa for personal, household, or family purposes.

188. As set forth herein, Wawa failed to protect Plaintiff and class members' Card Information due to data security failures, and misrepresented or omitted the nature of its inadequate data security policies and procedures.

189. Wawa's conduct and acts alleged herein constitute unfair or deceptive trade practices in violation of the D.C. CPPA Section 28-3904 in at least the following ways:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Washington, D.C. Class members' Card Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington, D.C. Class members' Card Information, including duties imposed by, *inter alia,* the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Washington, D.C. Class members' Card Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington, D.C. Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Washington, D.C. Class members' Card Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington, D.C. Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45.

190. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Card Information.

191. Defendant acted intentionally, knowingly, and maliciously to violate the D.C. CPPA, and recklessly disregarded Plaintiff and Washington, D.C. Class members' rights. Wawa's past data breaches discussed *supra*, and the multitude of recent, similar malware-based payment card breaches put it on notice that its security and privacy protections were inadequate.

192. Had Defendant disclosed to Plaintiff and Washington, D.C. Class members that its data systems were not secure and, thus, vulnerable to attack, Wawa would have been forced to adopt reasonable data security measures and comply with the law. Instead, it held itself out as a company that values data privacy, and it was entrusted with sensitive and valuable Card Information for millions of consumers, including Plaintiff and the Washington, D.C. Class members. Plaintiff and the Washington, D.C. Class members acted reasonably in relying on Wawa's misrepresentations and omissions, the truth of which they could not have discovered.

193. Wawa's unlawful trade practices were gross, oppressive, and aggravated, and it breached the trust of Plaintiff and the Washington, D.C. Class members.

194. As a direct and proximate result of Wawa's unlawful acts and practices, Plaintiff and Washington, D.C. Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; and increased, imminent risk of fraud and identity theft.

195. Plaintiff Lucas and Washington, D.C. Class members seek all monetary and nonmonetary relief allowed by law, including the greater of $1,500 per violation or treble damages for injury resulting from the direct and natural consequences of Wawa's unlawful conduct; injunctive relief; punitive damage; reasonable attorneys' fees and costs; and all other relief the Court deems proper.

COUNT IX
UNJUST ENRICHMENT
(On Behalf of Plaintiffs, the Nationwide Class, and all State Classes)

196. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

197. This claim is plead in the alternative to the above implied contract claim.

198. Plaintiffs and class members conferred a monetary benefit upon Wawa in the form of monies paid for the purchase of food and food-related services at its locations.

199. Wawa appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and class members. Wawa also benefited from the receipt of Plaintiffs' and class members' Card Information, as this was utilized by Wawa to facilitate payment to it.

200. The monies Plaintiffs and class members paid to Wawa were supposed to be used by Wawa, in part, to pay for adequate data privacy infrastructure, practices, and procedures.

201. As a result of Wawa's conduct, Plaintiffs and class members suffered actual damages in an amount equal to the difference in value between their purchases made with adequate data privacy and security practices and procedures that Plaintiffs and class members paid for, and those purchases without adequate data privacy and security practices and procedures that they received.

202. Under principals of equity and good conscience, Wawa should not be permitted to retain the money belonging to Plaintiffs and class members because Wawa failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

203. Wawa should be compelled to disgorge into a common fund for the benefit of Plaintiffs and class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

RELIEF REQUESTED

Plaintiffs, on behalf of all others similarly situated, request that the Court enter judgment against Defendant including the following:

A. Determining that this matter may proceed as a class action and certifying the Classes asserted herein;

B. Appointing Plaintiffs as representatives the applicable Classes and appointing Plaintiffs' counsel as class counsel;

C. An award to Plaintiffs and the Classes of compensatory, consequential, statutory, and treble damages as set forth above;

D. Ordering injunctive relief requiring Defendant to, e.g.,: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all class members;

E. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

F. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

G. Such other relief as the Court may allow.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury trial all issues so triable.

Dated: January 15, 2020

Respectfully submitted,

/s/ Benjamin F. Johns

Benjamin F. Johns
Samantha E. Holbrook
Andrew W. Ferich
Mark B. DeSanto
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Tel: (610) 642-8500
bfj@chimicles.com
seh@chimicles.com
awf@chimicles.com
mbd@chimicles.com

Sherrie R. Savett (PA Bar No. 17646)
Shanon J. Carson (PA Bar No. 85957)
Jon J. Lambiras (PA Bar No. 92384)
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103

Tel: (215) 875-3000
Fax: (215) 875-4604
ssavett@bm.net
scarson@bm.net
jlambiras@bm.net

E. Michelle Drake
BERGER MONTAGUE, PC
43 SE Main Street, Suite 505
Minneapolis, MN 55414
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Tina Wolfson
Bradley King
Henry Kelston
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com
bking@ahdootwolfson.com
hkelston@ahdootwolfson.com

William B. Federman
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Tel: (405) 235-1560
Fax: (405) 239-2112
WBF@federmanlaw.com

Jonathan Shub
William E. Hoese
Denis F. Sheils
Kevin Laukaitis
KOHN, SWIFT & GRAF, P.C.
1600 Market Street, Suite 2500
Philadelphia, PA 19103
Phone: (215) 238-1700
jshub@kohnswift.com
whoese@kohnswift.com
dsheils@kohnswift.com
klaukaitis@kohnswift.com

Melissa R. Emert
STULL, STULL & BRODY
6 East 45th St. 5th Floor
New York, NY 10017
Phone: (954) 341-55661
memert@ssbny.com

Marc D. Grossman
Andrei V. Rado
Blake Yagman
MILBERG PHILLIPS GROSSMAN, LLP
One Pennsylvania Plaza, Suite 1920
New York, NY, 10119-0165
Tel: (212) 594-5300
Fax: (212) 868-1229
mgrossman@milberg.com
arado@milberg.com
byagman@milberg.com

Counsel for Plaintiffs and the Classes